Counteracting Ambition: Applying Corporate Compliance and Ethics to the Separation of Powers Concerns with Domestic Surveillance[1]

Introduction

My first political memory is from 1974, when I was seven years old. I remember seeing a man on television, and to my young mind, something did not look right. I asked my father who the man was and what he was doing. My dad said the man was going to be the new President: It was August 9, 1974, and Gerald Ford was taking the oath of office of the President of the United States. I remember asking what happened to the old president. My dad told me that the old president had done some bad things and so he had to give up his job. My memory fades at that point, but my guess is that I probably said "OK" and went back to playing with my baseball cards.

I begin with this story because it identifies an important point of reference: I came of age in the post-Watergate era when limited and checked executive power was the norm, and suspicion—indeed, deep suspicion—of government officials was deemed the only prudent course. After all, this same era spawned the Office of the Independent Counsel,[2] a law barring bribery of foreign government officials,[3] and a law protecting the privacy of personal information held by the government.[4] The lesson was simple: When a government official says "trust me," it is best to do just the opposite.

This contrasts sharply with the view of some in the current administration. For example, Vice President Richard Cheney, who served in the federal government during the pre- and post-Watergate era,[5] believes that Watergate swung the pendulum too far against executive power, artificially cabining the President.[6] Not surprisingly, this has led to rather broad claims of executive power, such as unilateral executive power to indefinitely detain and try foreign enemy combatants[7] and to conduct domestic surveillance,[8] as well as presidential signing statements that ignore disagreeable provisions of federal statutes.[9]

Going forward, the challenge is to balance suspicion of and confidence in executive power—to leave the executive flexibility to

meet changing threats, while ensuring that flexibility is not a pretext for abuse. To begin answering this challenge, this Essay draws on expertise from an area of private law: the design, implementation, and operation of corporate compliance and ethics programs. A company's compliance and ethics program consists of the personnel, policies, and procedures that ensure employees and agents adhere to the company's legal and ethical obligations. For example, if a company has agents that do business overseas, it must address the concern that those agents might bribe foreign government officials to obtain business. The company should draft policies addressing payments to foreign government officials, train its agents on the relevant policies, monitor and audit its agents' expense statements, investigate suspicious activity, and discipline those who violate the policy.

My thesis is that constitutional separation of powers analysis ought to incorporate lessons from corporate compliance and ethics programs. Separation of powers requires adequate checks and balances to prevent abuse of federal power, and corporate compliance and ethics programs have proven powerful checks on the abuse of corporate power. Corporate compliance and ethics best practices, then, can guide analysis of whether a given exercise of federal power incorporates adequate checks against abuse.

This Essay uses the example of domestic foreign intelligence surveillance to develop its thesis. In December 2005, the *New York Times* reported that the Bush Administration had conducted a form of domestic surveillance, known as the Terrorist Surveillance Program (TSP), for about three years. Attorney General Alberto Gonzales explained that the TSP monitored communications where "one party [is] outside the United States" and the government has "a reasonable basis to conclude that one party to the communication is a member of al Qaeda, affiliated with al Qaeda, or a member of an organization affiliated with al Qaeda, or working in support of al Qaeda."[10] The Department of Justice claimed that both the President's inherent constitutional powers and federal law authorize such surveillance without judicial approval. After a federal district court struck down the program as violating the separation of powers and the Fourth Amendment,[11] the Bush administration agreed to seek federal court approval for future surveillance.[12]

While the TSP is now defunct, it raises ongoing concerns regarding government power and personal liberty. This Essay applies its separation of powers thesis to these concerns: When the government conducts domestic surveillance, it should protect citizen privacy by designing and implementing a compliance and ethics program. Federal law already requires many private companies that collect customer data to do so, and this Essay simply proposes that the federal government take a dose of its own medicine.[13]

This Essay has four parts. Part I reviews separation of powers first principles: Any program of domestic surveillance must satisfy these principles of checked and balanced power. Part II then describes the current dilemma posed by counter-terrorism—How to collect and analyze the mass of data needed to prevent the next terrorist attack while adequately protecting the privacy of United States citizens? Part III then describes how corporate compliance and ethics programs have allowed private companies to manage the risks posed by data privacy. Part IV concludes by arguing that separation of powers analysis ought to ask whether the federal government has adopted similar compliance and ethics measures when handling data collected for surveillance purposes.

I. Separation of Powers First Principles

This following discussion is *not* a summary or exposition of separation of powers doctrine. Rather, this Essay returns to the constitutional foundation, identifying first principles that underlie separation of powers analysis. The discussion does so through a series of quotes that capture the main points. The first three quotes are from James Madison's contributions to *The Federalist Papers*;[14] the next two quotes are from the Supreme Court's 2004 detainee decision in *Hamdi v. Rumsfeld*;[15] and the last two quotes are from Justice Robert Jackson's canonical concurrence in *Youngstown Sheet & Tube Co. v. Sawyer*.[16] Each quote is followed by observations about separating power among the three branches of the federal government.

"If men were angels, no government would be necessary."[17]

This truism is the root of all other separation of powers principles. Whether due to self-interest, prejudice, or some other human failing, society requires an organizing force to ensure order. And this

principle applies to the rulers as well as the ruled, for a "government of the people, by the people, and for the people"[18] will necessarily be "the greatest of all reflections on human nature."[19] Consequently, "[i]n framing a government which is to be administered by men over men, the great difficulty lies in this: you must first enable the government to control the governed; and in the next place oblige it to control itself."[20] This is an application of Lord Acton's Dictum: "Power tends to corrupt; absolute power corrupts absolutely."[21] The question is how best to get the government to "control itself."

"Ambition must be made to counteract ambition."[22]

This quote begins to answer how government might control the rulers—a form of intra-governmental divide and conquer. Later in the same passage, Madison elaborates on his point:

> [T]he great security against a gradual concentration of the several powers in the same department, consists in giving to those who administer each department the necessary constitutional *means* and personal *motives* to resist encroachments of the others. The provision for defense must in this, as in all other cases, be made commensurate to the danger of attack. . . . This policy of supplying, by opposite and rival interests, the defect of better motives, might be traced through the whole system of human affairs, private as well as public. We see it particularly displayed in all the subordinate distributions of power, where the constant aim is to divide and arrange the several offices in such a manner as that each may be a *check* on the other that the private interest of every individual may be a sentinel over the public rights.[23]

In short, government ought to be self-policing, and this plan had three parts. First, while "dependence on the people" for re-election will be the "primary safeguard" against tyranny, an essential "auxiliary precaution[]" is for each branch to check abuses of power by the other branches.[24] Hence the description of American government as one of checks and balances. Second, an effective system of checks requires that each branch have adequate "means"—that is, power—to check the other branches. For example, the executive can check legislative overreaching through the veto and the exercise of prosecutorial discretion. The legislature can check

executive ambition by overriding a presidential veto, controlling federal spending, or impeaching executive officials. Third, each branch must be given the "motive"—that is, an incentive—to use their powers to check the other branches.

"The accumulation of all powers, legislative, executive, and judiciary, in the same hands . . . may justly be pronounced the very definition of tyranny."[25]

This quote is a corollary of the preceding one: If all power is consolidated in the hands of a single branch, no other branch can check that branch's ambition. Without checks, we are back to absolute power and so tyranny. Yet, the danger of *all* government power ending up in the hands of a single branch is relatively small. The real threat is unchecked power over a specific subject, such as the treatment of those designated as unlawful enemy combatants.[26] While limited in scope, such power would be tyranny nonetheless.[27] So, this adage not only warns against collapsing government into a single branch, but urges vigilance against pockets of unchecked government power.

"[A] state of war is not a blank check for the President when it comes to the rights of the Nation's citizens."[28]

This principle anticipates a specific argument for consolidated federal power: "But we are at war!" Of course, war may provide a rationale for government action, or even justify deference to executive decisions. But war does not override the basic principle that each branch of government has limited, checked power.

"[T]he United States Constitution . . . most assuredly envisions a role for all three branches when individual liberties are at stake."[29]

This principle is a further corollary of the warning against consolidating government power. The President and Congress rarely claim sole power over a particular subject, but instead argue for great deference from the judicial branch. At times, this deference asks federal courts to simply accept, without scrutiny, a judgment of that branch. For example, the President has argued that federal courts should accept the executive's sole judgment as to whether

a person is an unlawful enemy combatant subject to trial before a military commission.[30]

Generally speaking, arguments for judicial deference are appropriate, as the judiciary must guard against accumulating too much power within its own hands (*i.e.*, tyranny of the judiciary). The case for deference, however, is weakest when individual liberties are at stake. Claims of individual liberties often arise in cases where an unpopular individual opposes the will of the popular branches of government, making protection in the political process unlikely. The federal judiciary, insulated from popular pressure by life tenure, is better situated to defend the rights of these unpopular individuals. Thus, the federal courts should carefully scrutinize arguments for judicial deference when individual liberties are at stake.

"[The Framers] suspected that emergency powers would tend to kindle emergencies."[31]

This principle is a specific application of the insight that government actors tend to seek expansion of their power. In *Youngstown Sheet & Tube Co. v. Sawyer*,[32] decided during the Korean War, President Truman argued that the Supreme Court ought to recognize implied emergency powers in the executive branch. Justice Jackson's concurring opinion noted that any such power was likely to expand with the imagination of whomever held the office. A President faced with no enumerated power to justify an action would simply declare an emergency. Justice Jackson's core insight is that federal courts ought to precisely and carefully define executive power, as the future tendency will be toward the most expansive application of that power.

"While the Constitution diffuses power the better to secure liberty, it also contemplates that practice will integrate the dispersed powers into a workable government."[33]

This last principle is itself a check on the preceding principles: Checks on government power ought not paralyze the government. The federal courts must be sensitive to the practical consequences of their doctrines. We want a government of checks *and balances*, with judicial review striking a realistic, workable balance.

II. The Threat to Liberty from Domestic Surveillance

Several commentators have noted that combating terrorism requires a different focus from conventional law enforcement.[34] While law enforcement takes a completed or ongoing action and asks who did it, counter-terrorism makes a predictive judgment—identify terrorists *before* they strike. To quote the 9/11 Commission, "terrorism cannot be treated as a reactive law enforcement issue, in which we wait until after the bad guys pull the trigger before we stop them."[35]

Judge Richard Posner notes that this shift from law enforcement to counter-terrorism enlarges the amount of data required by the government:

> [P]revention requires intelligence agencies to cast a much wider and finer-meshed net in fishing for information. Once a crime has occurred, a focused search for the criminal and for evidence of the crime is feasible. But if the concern guiding a search is that a crime might occur, the focus has to be much broader.[36]

This change makes probable cause and reasonable suspicion—traditional triggers for searches and seizures for domestic law enforcement—problematic. For requiring individualized suspicion, the argument goes, misses the very point of counter-terrorism surveillance: We do not know who they are or what they are planning.

To illustrate the breadth of counter-terrorism surveillance, consider the example of data-mining:

> Data mining is the process of looking for new knowledge in existing data. The basic problem addressed by data mining is turning low-level data, usually too voluminous to understand, into higher forms (information or knowledge) that might be more compact (for example, a summary), more abstract (for example, a descriptive model), or more useful (for example, a predictive model). At the core of the data mining process is the application of data analysis and discovery algorithms to enumerate and extract patterns from data in a database.[37]

Judge Posner describes the types of searches data-mining might include:

> Because of the volume involved, massive amounts of intercepted data must first be sifted by computers. The sifting can take two forms. One is a search for suspicious patterns or links; [for example,] searching for "use of a stolen credit card for a small purchase at a gas station—done to confirm whether a card is valid—before making a very significant purchase," a pattern suggestive of credit card fraud. The other form is the familiar Google-type search for more information about a known individual, group, subject, activity, identifier, and so on. A search for a social security number, for example, can reveal whether two similar or identical names are the names of two persons or one. The term "data mining" is sometimes limited to the first, the pattern search. But it is often used to embrace the second as well.[38]

While ordinary law enforcement begins with a known criminal act, and so might search a database by querying fields (such as name, address, social security number) for known information, counter-terrorism tries to prevent unknown events by unknown perpetrators, which makes the entire database potentially relevant. The challenge in data-mining is to analyze the underlying data using technologies that can reveal patterns and relationships that would otherwise go undetected.

To perform data-mining, the government must identify, collect, and aggregate data, which is no different from innumerable private firms that handle customer data:

> Because terrorist groups and affiliations are now global, because the number of potential terrorist targets is almost unlimited, because the variety of weaponry to which these groups may gain access is enormous, because modern surveillance technology can vacuum vast amounts of data, and because some terrorist groups are good at biding their time—which means that data from years ago may shed light on current and future terrorist schemes—the quantity of collectible data that may contain clues to terrorist plans or activities is immense, though not necessarily more immense than the data that commercial services handle more or less effortlessly.[39]

Similarly, private firms routinely analyze such data:

> To be assembled, retrieved, sorted, and sifted, so that patterns can be discerned and inferences drawn, intelligence data must be digitized, and the digitized data organized in databases linked to thousands of workstations (terminals, laptops, cellphones, in-vehicle displays, etc.) scattered throughout the intelligence system, not to mention tens of thousands of workstations elsewhere in the nation's farflung, poorly integrated, federal, state, local, and private security network. But that too is not unique.[40]

And like data collected by private firms, the government's data will be vulnerable to abuse or attack. Data could be improperly disclosed, either through inadvertence or misconduct of government personnel who handle the data, or through the wrongful acts of those who obtain unauthorized access to the data. Disclosure can cause harm through either embarrassment or the subsequent misuse of the information (*e.g.*, identity theft or blackmail). Also, the data could be abused by those with authorized access, as when the government targets its political opponents. And even legitimate use of the data can lead to false positives, as when an innocent person is mistakenly identified as a terrorist target.

The threats posed by domestic surveillance raise serious separation of powers concerns. Recall that when liberty is at issue, first principles counsel that the federal courts should play some role in checking abuses of government power. Here, the judiciary must play some role checking the abuses posed by data collection, analysis, and storage. Part IV argues that judicial review ought to examine whether the government's domestic surveillance programs implement an effective compliance and ethics program designed to reduce threats to data security. The next part describes what such a program entails.

III. Compliance and Data Privacy

This part links compliance and ethics programs to constitutional law. Section A describes the elements of an effective compliance and ethics program. Section B then explains how the 1977 case *Whalen v. Roe*[41] incorporated the concept of compliance and ethics into its constitutional analysis of database privacy.

A. Compliance Generally

All businesses take some measures to ensure that their employees and agents comply with applicable laws. After all, the simple directive to "be careful" is an informal attempt to comply with the negligence duty of care. Compliance and ethics programs formalize and expand upon these ad hoc efforts. The formality comes from designating personnel responsible for the compliance and ethics program, and implementing organizational infrastructures that carry out the various compliance and ethics functions. The expansion comes from a comprehensive attempt to identify and address the organization's legal risks and ethical principles.

Historically, businesses have had two main reasons to implement a compliance and ethics program. First, such programs hold the promise of reducing misconduct by both educating employees about their legal responsibilities and deterring potential wrongdoers. Compliance and ethics programs, then, are sensible when the expected reduction in liability costs exceeds the cost of implementing the program. Second, after prosecuting an organization for wrongdoing, the government has often required implementation of a compliance and ethics program. This occurred after industry scandals involving price fixing, insider trading, and health care fraud.

Over the last fifteen years, the incentives towards compliance have themselves become more formal. The trend began in 1991 when the United States Sentencing Commission promulgated organizational sentencing guidelines that mandated leniency for organizations that had an effective compliance and ethics program.[42] Since then, a variety of state and federal agencies have encouraged compliance and ethics programs through guidance or incentives. For example, the United States Department of Justice has directed United States Attorneys to consider either deferring or declining prosecution of organizations that have an effective compliance and ethics program.[43] In addition, an effective program can defend against civil vicarious liability for sexual harassment, commodities fraud,[44] or workplace safety violations.[45] And a recent wave of laws and regulations *require* compliance and ethics programs, making the program *itself* an aspect of complying with the law. The clear legal

trend is toward greater emphasis on private compliance and ethics programs.

While compliance and ethics programs cover a variety of risks and industries, they contain a basic set of elements regardless of the organization. The following ten steps are core requirements of an effective program:

1. Periodic risk assessments
2. Involvement of the organization's governing authority
3. Designating compliance personnel
4. Code of conduct
5. Written compliance and ethics standards
6. Employee and agent training
7. Lines of communication
8. Auditing and monitoring
9. Enforcement, discipline, and positive incentives
10. Periodic evaluation and improvement

In addition to these ten steps, the government expects an organization to foster an institutional culture that supports the compliance and ethics program. Even if all ten of the above compliance and ethics tasks are performed to the state-of-the-art, the program is doomed if employees and agents doubt the organization's sincerity. To return to a metaphor from the beginning of this section, if the risk assessment is the compliance and ethics program's blue print, then the organization's culture is the foundation.

B. Compliance and the Constitution: *Whalen v. Roe*

The Supreme Court's decision in *Whalen v. Roe*[46] illustrates how an ethics and compliance program (though the Court never called it that) can influence constitutional analysis. There, a New York law targeted diversion of drugs with legal uses "into unlawful channels."[47] For example, patients and physicians might use multiple or fake prescriptions to circumvent the state's drug control laws. To combat such abuse, one provision of the law prescribed record-keeping requirements for certain drugs:

> [A]ll prescriptions for [the specified] drugs [must] be prepared by the physician in triplicate on an official form. The completed form identifies the prescribing physician; the dispensing pharmacy; the drug and

> dosage; and the name, address, and age of the patient. One copy of the form is retained by the physician, the second by the pharmacist, and the third is forwarded to the New York State Department of Health in Albany. A prescription made on an official form may not exceed a 30-day supply, and may not be refilled.[48]

The database was supposed to reduce drug misuse in two ways. First, the state could analyze the data for patterns that indicated illegal use. Second, enhanced detection would deter misuse.

Similar to the data-mining described above, the New York database accumulated immense amounts of data concerning legitimate activity (here, legal drug prescriptions) to detect the few cases of illegal activity (here, drug abuse). For example, during the first twenty months that the database operated, the state collected an average of 100,000 prescription forms a month, and the data contributed to only two drug misuse investigations. This led the plaintiffs to characterize the database as "a vast state system that uses a dragnet more likely to expose the names of patients seeking drugs for legitimate medically indicated use than those obtaining drugs for illicit purposes."[49]

The plaintiffs, who were prescribed drugs covered by the record-keeping provision, argued that the database threatened harm due to misuse or disclosure of their data. Misuse could consist of the state stereotyping an individual in the database as a drug addict and discriminating against the person on that basis. Disclosure could occur either through a state employee leaking the information or an outsider gaining unauthorized access. These fears, in turn, allegedly discouraged patients from seeking needed medications. Note that these arguments parallel those regarding modern domestic surveillance: Centralized collection of data exponentially increases the harm posed by abuse of the data.

The Supreme Court upheld the database largely due to state-mandated controls that minimized the threat of abuse:

> [P]rescription forms are delivered to a receiving room at the Department of Health in Albany each month. They are sorted, coded, and logged and then taken to another room where the data on the forms is recorded on magnetic tapes for processing by a computer. Thereafter, the forms are returned to the receiving

> room to be retained in a vault for a five-year period and then destroyed as required by the statute. The receiving room is surrounded by a locked wire fence and protected by an alarm system. The computer tapes containing the prescription data are kept in a locked cabinet. When the tapes are used, the computer is run "off-line," which means that no terminal outside of the computer room can read or record any information. Public disclosure of the identity of patients is expressly prohibited by the statute and by a Department of Health regulation. Willful violation of these prohibitions is a crime punishable by up to one year in prison and a $2,000 fine.[50]

Here, one can glimpse aspects of an effective compliance and ethics program. For example, the state had a policy prohibiting the disclosure of patient information as well as specified punishment for a violation. Further, the Court saw evidence that the controls actually worked, as there was no evidence of problems with the New York database or similar databases in two other states. One would want to know, however, whether the state had other compliance functions, such as whether there was auditing or monitoring for violations of this non-disclosure rule.

The Court concluded its opinion by leaving open the question what role the existence of data security measures should play in future analysis:

> We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files. The collection of taxes, the distribution of welfare and social security benefits, the supervision of public health, the direction of our Armed Forces, and the enforcement of the criminal laws all require the orderly preservation of great quantities of information, much of which is personal in character and potentially embarrassing or harmful if disclosed. The right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures. Recognizing that in some circumstances that duty arguably has its roots in the Constitution, nevertheless New York's statutory scheme, and its implementing administrative proce-

> dures, evidence a proper concern with, and protection of, the individual's interest in privacy. We therefore need not, and do not, decide any question which might be presented by the unwarranted disclosure of accumulated private data whether intentional or unintentional *or by a system that did not contain comparable security provisions*. We simply hold that this record does not establish an invasion of any right or liberty protected by the Fourteenth Amendment.[51]

This passage yields two points relevant to the current analysis. First, in reviewing the constitutionality of government collection, analysis, and storage of citizen data, a court should consider what safeguards the government has implemented to prevent improper use or disclosure of the data. These safeguards are in essence compliance and ethics measures tailored to data security. Second, since *Whalen* was decided in 1977, the understanding and requirements of an effective compliance and ethics program in general, and for data security specifically, have changed dramatically. The next Part suggests that *Whalen*'s insight about the constitutional relevance of compliance measures be updated to take account of the increased formality and sophistication of modern compliance and ethics programs.

IV. Putting It All Together: A Separation of Powers Proposal

The preceding sections of this paper discuss aspects of the separation of powers, constitutional protections for private information, and compliance and ethic programs. The following discussion assimilates these observations into four propositions, and then offers a proposed tweak to our separation of powers analysis.

First, separation of powers requires some form of checks and balances among the three branches of the federal government. The checks and balances must be robust enough to prevent the accumulation of federal power in a single branch of government, even if that accumulation is in a narrow area. The need for checks and balances derives from human nature—those entrusted with government power will seek to expand their power.

Second, when the subject is individual liberty, it is important that the federal judiciary play a meaningful role in checking the power of the other two branches. This is because the popularly accountable

branches—the President and Congress—may not be adequately motivated to protect individual liberties, as when the claimed liberty is unpopular.

Third, modern domestic surveillance, even in aid of foreign intelligence, entails the collection and storage of massive amounts of private data concerning United States citizens. Citizens rightly fear that such data could be either misused or improperly disclosed, raising issues of individual liberty that (at times) may be unpopular. Separation of powers suggests that the federal judiciary ought to be involved in checking Congress and the President in this area. And *Whalen v. Roe* further suggests that one judicial check ought to be judicial review to determine whether the President and Congress have implemented adequate safeguards to prevent misuse or improper disclosure of private information.

Fourth, what is today called a corporate compliance and ethics program can provide needed safeguards against misuse or improper disclosure of private data. Since the Court decided *Whalen v. Roe* in 1977, the federal government, the states, and private industry have developed both general criteria for effective compliance and ethics programs, and specific criteria for data security programs. These criteria are specific enough for regulators, courts, and prosecutors to apply in determining whether a regulated entity has taken adequate compliance measures. Thus, separation of powers doctrine should incorporate modern compliance and ethics program standards. Specifically, courts should ask whether the President and Congress have established controls to prevent misuse or improper disclosure of private information of United States citizens collected and stored during domestic foreign intelligence surveillance.

A common objection to greater judicial review of federal anti-terrorism measures, and defense of greater judicial deference to the President and Congress, is the courts' comparative lack of expertise in the area. As Judge Posner has put it, "[j]udges aren't *supposed* to know much about national security."[52] One need not dispute this claim to endorse this paper's proposal. First, as discussed above, strong consensus exists among regulators and private firms about the essential components of an effective compliance and ethics program. Of course, there is discussion and debate regarding some details, such

as whether the corporate compliance officer ought to report through the organization's legal department or directly to the CEO or a board committee. But courts can apply the consensus standards and give deference where consensus runs out.

Second, we know that evaluating compliance and ethics programs is not beyond judicial competence because courts already do so in several contexts. As discussed above, the United States Sentencing Guidelines direct federal courts to assess the effectiveness of a corporate defendant's compliance and ethics program as a mitigating factor in criminal sentencing. In federal sexual harassment and civil rights cases, federal courts assess a corporate defendant's compliance and ethics program in litigating a defense to vicarious liability.[53] Under state corporate law, recent decisions from the Delaware Supreme Court suggest that that state's courts will now assess whether a corporate board has adhered to compliance best practices in ruling on a motion to dismiss claims against directors.[54] And courts and agencies are increasingly incorporating compliance and ethics efforts into legal tests. It is far too late in the day to claim that evaluating compliance and ethics programs is beyond judicial competence.

The remaining question is whether corporate compliance and ethics measures ought to be a safe harbor or a constitutional requirement. Here, Justice Jackson's admonition looms large: "While the Constitution diffuses power the better to secure liberty, it also contemplates that practice will integrate the dispersed powers into a workable government."[55] This counsels a safe harbor approach for three reasons. First, while corporate compliance and ethics programs have proven effective at checking private misconduct, they may not be the only (or even best) measure for checking abuse of government power. Consequently, this Essay's modest proposal ought to proceed modestly, recognizing the inherent limits of human knowledge.

Second, even a safe harbor can have a powerful incentive effect. This is because a safe harbor provides the certainty of a specific outcome—here, constitutionality—whereas alternative measures offer uncertainty. Further, this safe harbor holds the benefit of identifiable criteria that provide concrete guidance for government action. In designing and implementing a compliance and ethics

program to protect citizen data, the federal government can benchmark against private entities that must perform the same tasks for private customer data. Indeed, in some instances the federal government will be analyzing data obtained from private databases that are themselves legally required to have data security compliance and ethics programs.

Third, judges will be more timid in identifying and applying compliance and ethics principles if doing so poses a constitutional bar to government action. As Judge Posner has written:

> Judges, knowing little about the needs of national security, are unlikely to oppose their own judgment to that of the executive branch, which is responsible for the defense of the nation. They are especially unlikely to interpose *constitutional* objections because of the difficulty of amending the Constitution to correct judicial error.[56]

The safe harbor frees judges to rule definitively on compliance and ethics principles, knowing that the federal government may experiment with alternate arrangements.

To summarize, this Essay proposes the following separation of powers analysis. When the federal government collects private information of United States citizens while conducting foreign intelligence surveillance, separation of powers demands that adequate checks and balances protect against abuse or misuse of the information. The government may carry this burden by demonstrating that its data collection, analysis, and storage operate under an effective compliance and ethics program. If the government does not carry this burden, it must then show that its surveillance includes internal controls with the same level of protection provided by an effective compliance and ethics program.

Conclusion

Throughout American history, the Supreme Court has applied the Constitution to changed circumstances. After 9/11, the Court must do so again as some battles in the war on terror threaten our constitutional commitment to liberty and privacy. While the Bill of Rights often takes center stage when individual liberty is threatened, we must not forget that separation of powers—our system of checks

and balances—is the first line of defense against such incursions. Our timeless commitment to separated power must now be applied to the federal government's efforts to identify terrorists and prevent their attacks. This Essay proposes that separation of powers analysis look to the evolving discipline of corporate compliance and ethics for guidance. Over the last half century, businesses have accumulated vast expertise on checking and balancing the exercise of private authority to protect shareholder value. The federal government ought to employ similar measures to protect our constitutional values.

Endnotes

1 This essay extends my remarks delivered at the conference "Guarding the Guardians: The Ethics and Law of Domestic Surveillance," hosted by the Cary M. Maguire Center for Ethics and Professional Responsibility at Southern Methodist University on October 20, 2006. I thank my co-presenters for their comments and questions on my presentation. Also, special thanks to Professor Thomas Mayo, Director of the Maguire Center, for the invitation to participate in the event.

2 28 U.S.C. § 595 (2005).

3 *Foreign Corrupt Practices Act*, 15 U.S.C. §§ 78dd-1, et seq. (2005).

4 *Privacy Act*, 5 U.S.C. § 552a (2005).

5 Vice President Cheney served as President Ford's Chief of Staff. See The White House, Vice President Richard B. Cheney, http://www.whitehouse.gov/vicepresident/.

6 See Michiko Kakutani, "The Case Against Those Expanding White House Powers," *New York Times*, July 6, 2007, E32 ("[E]xpanded executive power was not a response to the terrorist attacks of 9/11 but the realization of a vision that conservatives like Dick Cheney had harbored since the 1970s, when they grew aggrieved over post-Watergate reforms that put the brakes on presidential power."). Vice President Cheney had endorsed these same views in 1987 when, as representative of the State of Wyoming, he joined the Minority Report on the Iran Contra Affair. See *Report of the Congressional Committees Investigating the Iran-Contra Affair*, H.R. Rep. No. 100-433, (1987): 457-58.

7 See *Hamdi v. Rumsfeld*, 542 U.S. 507, 535-36 (2004) (addressing the administration's argument regarding detainees that "the courts must forgo any examination of the individual case and focus exclusively on the legality of the broader detention scheme").

8 See U.S. Department of Justice, *Legal Authorities Supporting the Activities of the National Security Agency Described by the President* (Jan. 19, 2006), available at http://www.usdoj.gov/opa/whitepaperonnsalegalauthorities.pdf.

9 See American Bar Association, *Task Force on Presidential Signing Statements and the Separation of Powers Doctrine* (Aug. 2006), 14-18. This report discusses the second Bush administration's use of presidential signing statements, available at http://www.abanet.org/op/signingstatements/aba_final_signing_statements_recommendation-report_7-24-06.pdf.

10 Press Briefing by Attorney General Alberto Gonzales and General Michael Hayden, Principal Deputy Director for National Intelligence, Dec. 19, 2005, available at http://www.whitehouse.gov/news/releases/2005/12/20051219-1.html.

11 *A.C.L.U. v. National Sec. Agency*, 438 F. Supp. 2d 754 (E.D. Mich. 2006), *rev'd on other grounds*, 2007 WL 1952370 (6th Cir. July 6, 2007).

12 Letter from Attorney General Alberto R. Gonzales to Hon. Patrick Leahy and Hon. Arlen Spector, dated Jan. 17. 2007, available at http://graphics8.nytimes.com/packages/pdf/politics/20060117gonzales_Letter.pdf.

13 After I had presented this paper, the Department of Justice announced that it was implementing additional internal controls over its national security activities. See Letter from Alberto Gonzales to Richard B. Cheney, dated July 13, 2007, available at http://www.justice.gov/opa/pr/2007/July/cheney_letter071307.pdf; Press Release, Federal Bureau of Investigation, "Justice Department and FBI Unveil Measures to Enhance National Security Oversight," July 13, 2007 ("While compliance programs have long been a staple of private corporations, this effort would represent one of the first times a federal agency established an agency-wide compliance program."), available at http://www.justice.gov/opa/pr/2007/July/07_nsd_498.html.
14 *The Federalist Papers No. 51* (Madison), available at http://thomas.loc.gov/home/histdox/fed_51.html
15 542 U.S. 507 (2004).
16 343 U.S. 579 (1952).
17 *The Federalist Papers No. 51* (Madison).
18 Gettysburg Address, dedication of the Soldiers' National Cemetery in Gettysburg, Pennsylvania, on November 19, 1863.
19 *The Federalist Papers No. 51* (Madison).
20 Ibid.
21 Letter from John Dahlberg-Acton to Bishop Mandell Creighton, dated Apr. 1887 (referring to the doctrine of papal infallibility in the Catholic Church), reprinted in *The New Dictionary of Cultural Literacy*, 3rd edition, ed. by E.D. Hirsch, Jr., Joseph F. Kett, and James Trefil (Boston: Houghton Mifflin, 2002).
22 *The Federalist Papers No. 51* (Madison).
23 Ibid. (emphasis added).
24 Ibid.
25 *The Federalist Papers No. 47* (Madison).
26 *Hamdan v. Rumsfeld*, 126 S. Ct. 2749, 2780 (2006).
27 See *Clinton v. City of New York*, 524 U.S. 417, 450 (1998) (Kennedy, J., concurring) (striking down the Line Item Veto Act as a violation of separation of powers).
28 *Hamdi v. Rumsfeld*, 542 U.S. 507, 536 (2004).
29 Ibid.
30 Ibid.
31 Y*oungstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 650 (1952) (Jackson, J., concurring in the judgment and opinion of the Court).
32 Ibid.
33 Ibid., 635.
34 See, e.g., Richard A. Posner, *Not a Suicide Pact: The Constitution in a Time of National Emergency* (Oxford University Press, 2006).
35 Editorial, "The Limits of Hindsight," *WALL ST. J.*, July 28, 2003, A10.
36 Posner, *Suicide Pact*, 92-93.
37 K. A. Taipale, *Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data*, 5 Colum. Sci. & Tech. L. Rev. 2 (2003).
38 Posner, *Suicide Pact*, 96-97.

39 Richard A. Posner, *Uncertain Shield: The U.S. Intelligence System in the Throes of Reform* (Rowman & Littlefield Publishers, 2006), 141 .
40 Ibid., 141-42.
41 429 U.S. 589 (1976).
42 Amendments to the Sentencing Guidelines for United States Courts, 56 Fed. Reg. 22,762 (May 16, 1991).
43 Memorandum from Paul J. McNulty, Deputy Attorney General, to Heads of Department Components and United States Attorneys, 12-15, available at http://www.usdoj.gov/dag/speech/2006/mcnulty_memo.pdf.
44 See *Commodity Futures Trading Comm'n v. Carnegie Trading Group, Ltd.*, 450 F. Supp. 2d 788, 804-05 (N.D. Ohio 2006).
45 See *W.G. Yates & Sons Constr. Coo., Inc. v. OSHA*, 459 F.3d 604, 608-09 (5th Cir. 2006).
46 429 U.S. 589 (1977).
47 Ibid., 591.
48 Ibid., 593.
49 Ibid., 17. The appellees also challenged the efficacy of the database. For example, while a search of the records would identify a person who obtained multiple prescriptions under the same name, it could not detect a person who used an alias to obtain the prescriptions.
50 Ibid., 593-94.
51 Ibid., 605-06 (emphasis added).
52 Posner, *Suicide Pact*, 37.
53 See *Kolstad v. American Dental Ass'n*, 527 U.S. 526 (1999) (good faith compliance efforts can be a defense to punitive damages liability in federal civil rights action); *Burlington Indus., Inc. v. Ellerth*, 524 U.S. 742 (1998) (reasonable efforts to detect and remedy incidents of sexual harassment can be defense to employer liability); *Faragher v. City of Boca Raton*, 524 U.S. 775 (1998) (same).
54 See *Stone v. Ritter*, 911 A.2d 362 (Del. 2006); In re *Caremark Int'l Inc. Derivative Litig.*, 698 A.2d 959 (Del. Ch. 1996).
55 *Youngstown*, 343 U.S. at 635 (Jackson, J., concurring in the judgment and opinion of the Court).
56 See Posner, S*uicide Pact*, 9.

THE CARY M. MAGUIRE CENTER FOR ETHICS AND PUBLIC RESPONSIBILITY

The leaders of Southern Methodist University believe that a university does not fully discharge its responsibility to its students and to the community at large if it hands out knowledge (and the power which that knowledge eventually yields) without posing questions about its responsible uses. Through the Cary M. Maguire Center for Ethics and Public Responsibility, SMU strives to foster the moral education and public responsibilities of those whom it empowers by:

- Supporting faculty research, teaching, and writing in ethics that cross disciplinary, professional, racial/cultural, and gender lines;
- Strengthening the ethics component in SMU's undergraduate and professional curriculum;
- Awarding grants to SMU students who wish to study issues in ethics or engage in community service.

SMU also believes that a university and the professions cannot ignore the urban habitat they helped to create and on which they depend. Thus, while not an advocacy group, the Maguire Center seeks to be integrally a part of the Metroplex, attending to the moral quandaries and controversies that beset our common life. To that end, the Center:

- Has created an Ethics Center Advisory Board of professional and community leaders;
- Organizes local seminars, colloquia, and workshops featuring SMU and visiting scholars;
- Publishes occasional papers and books based on the Center's endeavors that will be of interest to both academics and the general public.

FOR MORE INFORMATION:

Cary M. Maguire Center for Ethics and Public Responsibility
Southern Methodist University
PO Box 750316
Dallas, TX 75275-0316
214-768-4255
www.smu.edu/ethics_center

Any of the occasional papers may be obtained from the Maguire Center for Ethics and Public Responsibility for $2 per paper. Please make checks payable to SMU.